Virginia Information Technologies Agency

Commonwealth Information Security Officers Advisory Group (ISOAG) Meeting

January 8, 2008

Happy New Year!

2 0 0 8 !

Happy New Year!

VITA Virginia Information Technologies Agency

ISOAG January 2008 Agenda

I.	Welcome and Opening Remarks	Peggy Ward, (VITA)
II.	Information Technology Governance in the Commonwealth	Karen Helderman, (APA)
III.	Document Management Initiative Update	Herb Ward, (DEQ)
IV.	The Commonwealth of Virginia Knowledge Center, Overview	Belchoir Mira, (DHRM)
V.	Data Removal Standard	Cathie Brown (VITA)
VI.	Commonwealth Information Security Annual Report	Cathie Brown (VITA)
VII.	Wireless Threat Environment	Tripp Sims (VITA)
VIII.	Upcoming Events & Other Business	Peggy Ward, (VITA)

Information Technology Governance

APA

Auditor of Public Accounts

COMMONWEALTH OF VIRGINIA

Karen Helderman

January 2008

Objectives of Our Review

To determine whether:

- effective IT governance exists for all areas where the Commonwealth spends money on information technology.
- the Commonwealth’s current IT governance follows best practices.
- risks exist within the Commonwealth as a result of the current IT governance structure.

Who Has Control?

- VITA controls the infrastructure.
- CIO and ITIB control new systems development recommendations.
- Individual agencies control maintenance and operations of legacy applications.
- Governor controls budget process.

Answer to Who Has Control

Nobody

- Control is decentralized and responsibilities are divided among many entities with no one entity having control or authority to make decisions.

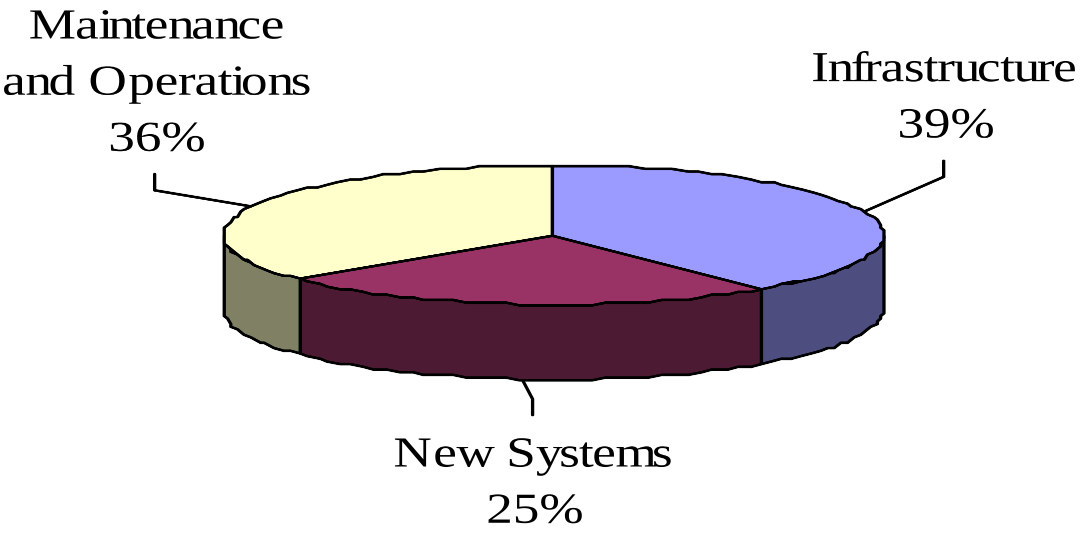
Effects of Lack of Control

No one determines if spending is made most efficiently resulting in duplication, lack of sound investment, and systems development projects that do not support COVA’s business plan.

Effects of Lack of Control

- Examples:
  - State official added language to an agency’s RFP for a new system to include outsourcing the infrastructure.
  - Assumption that Governor and General Assembly would not fund system modernizations led to expensive conversions that are short term fixes.
  - Failure to successfully implement an enterprise licensing system.
  - Lack of data standards has led to disparate systems that cannot share information.
  - Agencies developing systems with maintenance & operating funds
  - Agency new systems rate of return showed only 1.97%.

Breakdown of Annual Spending



IT Governance in COVA

- $238 million annually represents payments to VITA for providing the infrastructure. The infrastructure is owned and managed by VITA/NG.
- $150 million annually represents new systems development projects and IT governance structure exists through statutes (creating the ITIB and CIO) and PMD defined standards.

IT Governance in COVA

- $219 million annually represents agencies spend on maintenance and operations of legacy applications. Control over what these funds are used for and how they are used is an individual agency decision. No comprehensive review of whether this could be spent more efficiently. Also, some agencies lack technical experts.

IT Governance Best Practices

- IT Governance Institute has created COBIT and Val IT, both of which represent industry best practices over IT governance.
- COBIT focuses on are managing our IT resources the right way and are we managing them well.
- Val IT focuses on the IT investment decision process and are we doing the right things and are we realizing the benefits.

IT Governance Best Practices

- Val IT suggests that all IT spending, including the infrastructure, new systems development projects, and maintenance and operations of legacy systems, be subject to an IT investment decision making process.
- Val IT is about planning and implementing IT investment decisions to optimize the value to the enterprise.

IT Governance Best Practices

- Val IT contains 40 key management practices such as:
  - The business and IT strategy should be integrated, clearly linking the enterprise goals and IT goals and should be broadly communicated.
  - Create and maintain an inventory of current IT human resources, their competencies, and their current and committed utilization.
  - Prepare a program budget that reflects the full economic life cycle costs and financial and non-financial benefits, and submit for review, refinement, and approval by the business sponsor.

Comparison of COVA IT Governance to Best Practices

- We compared COVA's IT governance for the infrastructure, new systems , and maintenance and operations to the 40 Val IT key management practices and found the following:
- IT governance over infrastructure is transforming.
- IT governance over new systems is maturing.
- IT governance over maintenance and operations is non-existent.

Comparison of COVA IT Governance to Best Practices

- Each IT spending area has different processes for approval and funding.
- Many entities control various pieces of the process with no one entity determining the overall direction or overseeing spending.
- ITIB has discussed how to improve visibility over what agencies spend on IT and improving IT investments, but realize they do not have the authority to collect data or enforce compliance.

Conclusion

- There is a relationship between all three IT spending areas and all need sound IT governance practices.
- Opportunities exist to improve IT spending across all areas and reduce the current silo approach.
- Many of COVA’s IT governance problems result from the disparate processes used to provide governance and the lack of central planning, investment, control and monitoring.

Recommendations

- Improve agency IT budget request detail and provide authority for oversight.
- Collect information in the Portfolio (Prosight).
- Provide for an Office of the CIO or funding for ITIB activities.
- Review IT funding and budget model for small and medium sized agencies.

Recommendations

- Delegate data standard responsibilities and require new systems to conform.
- Provide new systems development budgets in a manner similar to capital outlay.
- Provide General fund moneys for project management policy.
- Finalize Northrop Grumman procedures manual to include on-going governance.

A complete copy of the report can be found at

www.apa.virginia.gov

Questions?

Document Management Initiative Update

H. R. Ward

DEQ

Acronyms, Synonyms, etc.

- Document Management (DM)
- Enterprise Content Management (ECM)
- Records Management (RM)
- Web Content Management (WCM)

Background

- October 2006 – ITIB directs DEQ to lead Enterprise Document Management effort to establish Commonwealth contracts for document Management as part of Governor’s Paperless Government Initiative
- June 2007 – ECM software contract awarded and IBM FileNet designated as Commonwealth ECM standard
- November 2007 – ECM Implementation Services Contract awarded to:
  - BearingPoint
  - CGI-AMS
  - HCL America
  - IMC
- October 2007 - Paperless Government Initiative oversight by VA Enterprise Applications Project (VEAP)

Next Steps

- DEQ to start Agency implementation in late January
- ECM “Governance” effort moving forward
  - Commonwealth ECM Center of Excellence
  - Reusable Components
  - Shared Services

Shared Services?

- LVA to host a shared services environment for smaller agencies
  - LVA to provide administration
  - Agencies to purchase licenses and maintenance
  - Designed for ~200 users

Contact Information

H. R. Ward
VA Department of Environmental Quality
Office of Information Systems
hrward@deq.virginia.gov
804.698.4316

DEQ ECM Implementation questions:
Bernie Farkas
bwfarkas@deq.virginia.gov
804.698.4386

Commonwealth of Virginia
Knowledge Center

Commonwealth of Virginia Knowledge Center Overview

Belchior Mira
Chief Information Officer
Department of Human Resource Management

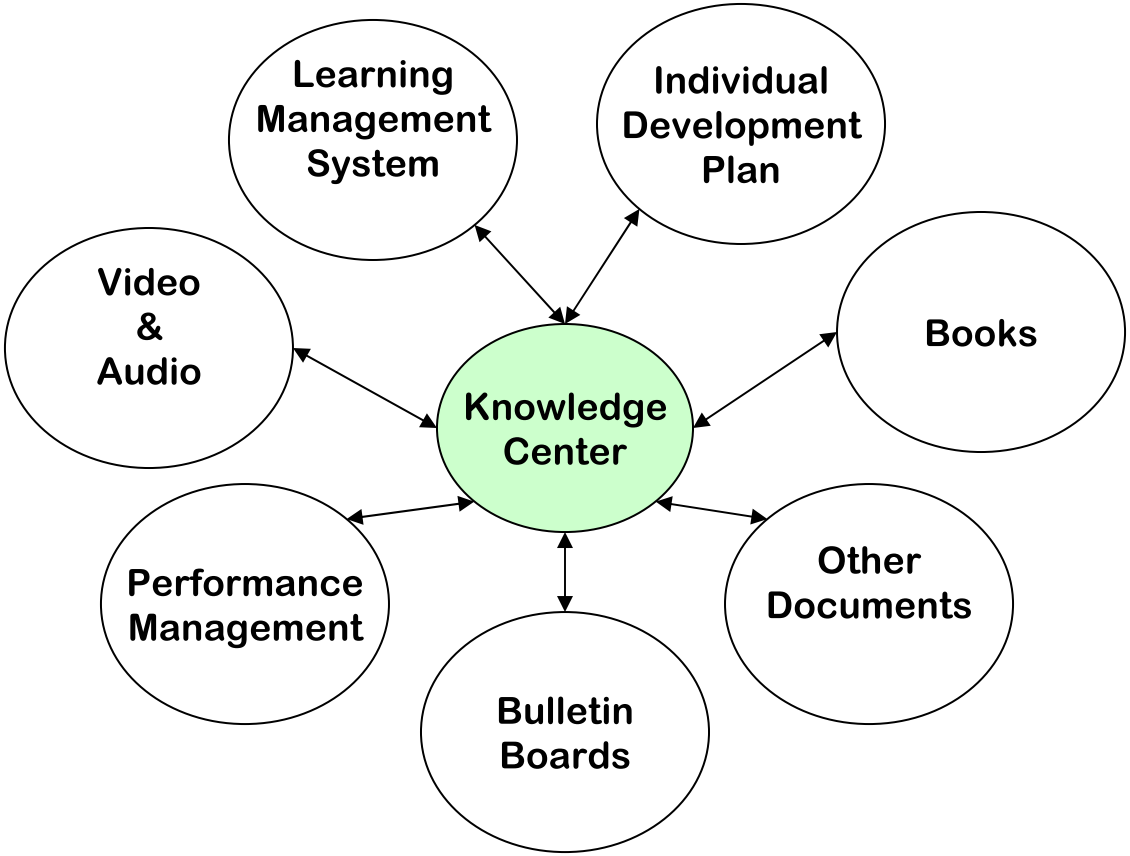
- Introduction
- Assessment
- Implementation
- Conclusion
- Questions
- Demo

Commonwealth Knowledge Center

- Web-Based Enterprise Solution
  - Owned by the Commonwealth of Virginia
  - Hosted by Meridian Knowledge Solutions, LLC

- Manages the Administration of Training
- Benefits any agency in state government and any other public body
- Allows consolidation and integration of different learning management systems
- Allows different approaches for implementation of different portals

Commonwealth Knowledge Center



Learning Management System

Individual Development Plan

Video & Audio

Knowledge Center

Books

Performance Management

Other Documents

Bulletin Boards

Learning Management System

More specifically …

- A learning management system (LMS) is a Web-based technology used to plan, implement, and assess a specific learning process.
- It includes functionality for course catalogs and assessments.
- It provides an instructor with a way to create and deliver content, monitor student participation, and assess student performance.
- It provides students with the ability to register on-line for or launch courses, track progress, use interactive features such as threaded discussions, video conferencing, and discussion forums.

Participating State Agencies and Other Public Bodies

1. CNU – Christopher Newport University – (Evaluation)
2. DBVI - Department for the Blind and Vision Impair – (Evaluation)
3. DDHH - Department for the Deaf and Hard of Hear – (Evaluation)
4. DCE - Department of Correctional Education – (LIVE)
5. DCJS – Department of Criminal Justice Services – (Evaluation)
6. DCR - Department of Conservation and Recreation – (Implementation)
7. DEDR - Department of Employment Dispute Resolution - (LIVE)
8. DEQ – Department of Environmental Quality – (Implementing)
9. DFP – Department of Fire Programs – (Implementing)
10. DGIF – Department of Game & Inland Fisheries (Implementation)
11. DGS - Department of General Services – (LIVE)
12. DGS/DPS - Division of Purchases & Supply (LIVE)
13. DHCD - Department of Housing and Community Development - (Implementation)
14. DHRM - Department of Human Resource Management – (LIVE)
15. DJJ - Department of Juvenile Justice - (LIVE)
16. DMAS - Department of Medical Assistance Services (Implementation)
17. DMHMRSAS (CATAWBA) - Catawba Hospital – (Evaluation)
18. DMHMRSAS (CCCA) - COV Center for Child & Adolescents – (Evaluation)
19. DMHMRSAS (CO) - Central Office - (Evaluation)
20. DMHMRSAS (CSH) - Central State Hospital – (Evaluation)

Participating State Agencies and Other Public Bodies

21. DMHMRSAS (CVTC) - Central Virginia Training Center – (Evaluation)
22. DMHMRSAS (CFS) - Child & Family Services – (Evaluation)
23. DMHMRSAS (ESH) - Eastern State Hospital – (Evaluation)
24. DMHMRSAS (HWDMC) - Hiram W. Davis Medical Center – (Evaluation)
25. DMHMRSAS (NVMHI) – Northern Va. Mental Health Institute – (Implementing)
26. DMHMRSAS (NVTC) - Northern Virginia Training Center – (Evaluation)
27. DMHMRSAS (OFO) - Office of Facility Operations – (Evaluation)
28. DMHMRSAS (OL) - Office of Licensing – (Evaluation)
29. DMHMRSAS (OMH) - Office of Mental Health – (Evaluation)
30. DMHMRSAS (OMR) - Office of Mental Retardation – (Evaluation)
31. DMHMRSAS (OMRPC) - Office of Mental Retardation Providers & Community
32. DMHMRSAS (OQM) - Office of Quality Management – (Evaluation)
33. DMHMRSAS (PGH) - Piedmont Geriatric Hospital – (Evaluation)
34. DMHMRSAS (SEVTC) - Southeastern Virginia Training Center – (Evaluation)
35. DMHMRSAS (SVMHI) - Southern Virginia Mental Health Institute – (Evaluation)
36. DMHMRSAS (SVTC) - Southside Virginia Training Center – (Evaluation)
37. DMHMRSAS (SWVMHI) - Southwestern Virginia Mental Health Institute – (Evaluation)
38. DMHMRSAS (SWVTC) - Southwestern Virginia Training Center – (Evaluation)
39. DMHMRSAS (VCBR) - Virginia Center for Behavioral Rehabilitation (Evaluation)
40. DMHMRSAS (WSH) - Western State Hospital – (Evaluation)

Participating State Agencies and Other Public Bodies

41. DMV - Department of Motor Vehicles - (LIVE)
42. DOA - Department of Accounts – (Implementation)
43. DOE - Department of Education – (Evaluation)
44. DOF - Department of Forestry – (Implementation)
45. DPB - Department of Planning and Budget – (Implementation)
46. DRS - Department of Rehabilitative Service – (Implementing)
47. DRS (DDS) - Disability Determination Services - (Evaluation)
48. DSS - Department of Social Services - (Implementation)
49. DVS - Department of Veteran Services – (LIVE)
50. LVA – The Library of Virginia – (Implementation)
51. JSRCC – J. Sargent Reynolds Community College - (Evaluation)
52. VADOC - Va. Department of Corrections (includes 31 facilities) – (LIVE)
53. VATAX - Va. Department of Taxation – (LIVE)
54. VATRS – Va. Department of the Treasury - (Implementation)
55. VDEM – Va. Department of Emergency Management - (Evaluation)
56. VDOT - Va. Department of Transportation – (LIVE)
57. VEC - Va. Employment Commission - (LIVE)
58. VHDA - Va. Housing Development Authority – (LIVE)

Participating State Agencies and Other Public Bodies

59. VITA - Va. Information Technologies Agency – (LIVE)
60. VSBE - Va. State Board of Elections – (Evaluation)
61. VSDB – Va. School for the Deaf and the Blind - Staunton - (Evaluation)
62. VSP - Va. State Police - (LIVE)
63. VSU - Virginia State University (Evaluation)
64. VWC – Virginia Workers Compensation - (Evaluation)
65. VRCB – Virginia Rehabilitation Center for the Blind
66. VWCC – Virginia Western Community College (LIVE)
67. WWRC - Woodrow Wilson Rehab Center (Evaluation)
68. VBPD - Virginia Board for People with Disabilities

Assessment

Consolidation

- Platforms
- Software
- Vendors
- Budget
- Content
- User profiles
- User transcripts

Consolidation

- Savings
- Efficiency
- Effectiveness
- Training

Implementation

Assumptions

- Ownership
- Identity
- Independency
- Configurability

Assurances

- One Enterprise Statewide System
- Multiple Portals
- Content management
- One user profile
- One transcript

One Statewide Enterprise System
– Multiple Portals -

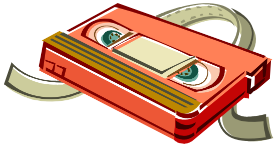
VDOT UNIVERSITY
VIRTUAL CAMPUS
dhrm
Knowledge Center
VITA
KNOWLEDGE CENTER
VIRGINIA DEPARTMENT OF EDUCATION
DGS
Agency of Choice
ASD
DCE
Log In to the DCE Knowledge Center
Virginia State Police
Virtual University
Commonwealth of Virginia
Knowledge Center
VIRGINIA WESTERN
The Community's College
Knowledge Center
Virginia Department of Juvenile Justice
Knowledge Center
Virginia Employment Commission
Your Link to Learning
DMV
Knowledge Center
Virginia Department of
socialservices
VHDA University
VA
TAX Knowledge Center
Virginia State Board of Elections
Department of Veterans Services
Online Training Center

Content Management

- Content sharing
- Domain Manager
- Team Rooms

Content Sharing

- All Domains
- Select Domains
- Privacy
- Confidentiality
- Accessibility



Conclusion

Conclusion

- Consolidates and integrates different learning management systems actually in-place accomplishing significant savings

- Reduces cost associated with training

- Reduces or complete eliminates duplication of training content developed and/or purchased

- Facilitates statewide initiatives by expediting the process of statewide training on major policy changes

- Promotes fairness and equity - accessible to all state employees and other individuals that participate in public entities training

- Increases the effectiveness and efficiency of the training provided to the workforce.

Conclusion

- ➢ Training available on demand, any time, anywhere

- ➢ Reduces or complete eliminates the duplication of training developed and/or purchased

- ➢ Consolidation and integration of different learning management systems actually in-place accomplishing significant savings

- ➢Facilitates statewide initiatives by expediting the process of statewide training on major policy changes and initiatives

- ➢ Promotes fairness and equity by being accessible to all state employees and other individuals that participate in public entities training

- ➢ Reduction in cost associated with training increasing the effectiveness and efficiency of the service provided to the workforce.

Commonwealth of Virginia
Knowledge Center

Questions

Belchior Mira - Knowledge Center Project Manager

Brooke Schepker – Knowledge Center System Administrator
for the Commonwealth

covkcadmin@dhrm.virginia.gov

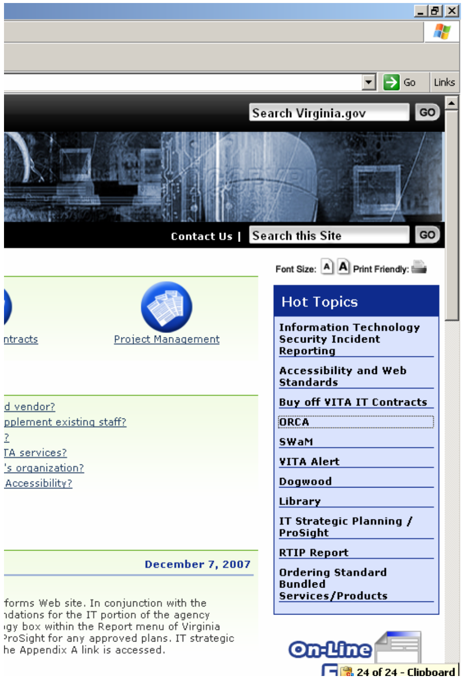
VITA Virginia Information Technologies Agency

Removal of Commonwealth Data from Electronic Media Standard

Cathie Brown, CISM, CISSP
Deputy Chief Information Security Officer

Removal of Data Standard - Status

- Posted to ORCA (Online Review and Comment Application)



Hot Topics

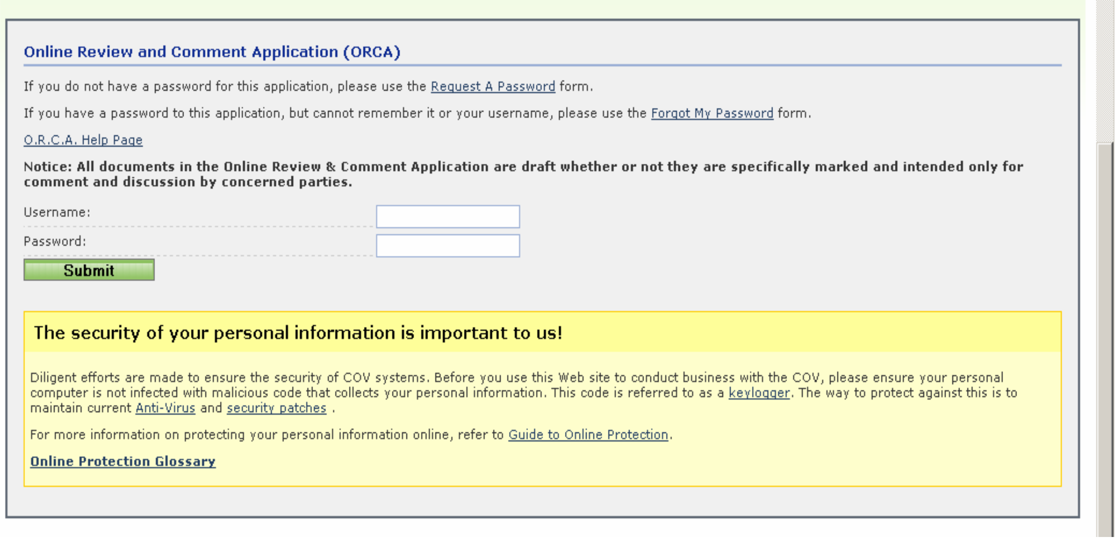
- Information Technology Security Incident Reporting
- Accessibility and Web Standards
- Buy off VITA IT Contracts
- ORCA
- SWaM
- VITA Alert
- Dogwood
- Library
- IT Strategic Planning / ProSight
- RTIP Report
- Ordering Standard Bundled Services/Products

d vendor?
pplement existing staff?
?
TA services?
's organization?
Accessibility?

December 7, 2007

forms Web site. In conjunction with the
ndations for the IT portion of the agency
gy box within the Report menu of Virginia
ProSight for any approved plans. IT strategic
he Appendix A link is accessed.

http://www.vita.virginia.gov/



Online Review and Comment Application (ORCA)

If you do not have a password for this application, please use the Request A Password form.

If you have a password to this application, but cannot remember it or your username, please use the Forgot My Password form.

O.R.C.A. Help Page

Notice: All documents in the Online Review & Comment Application are draft whether or not they are specifically marked and intended only for comment and discussion by concerned parties.

Username:

Password:

Submit

The security of your personal information is important to us!

Diligent efforts are made to ensure the security of COV systems. Before you use this Web site to conduct business with the COV, please ensure your personal computer is not infected with malicious code that collects your personal information. This code is referred to as a keylogger. The way to protect against this is to maintain current Anti-Virus and security patches .

For more information on protecting your personal information online, refer to Guide to Online Protection.

Online Protection Glossary

http://apps.vita.virginia.gov/publicORCA/default.asp

Data Removal Standard – Scope

- Applies to ALL State Agencies
  - – Applicable to the Commonwealth's executive, legislative, and judicial branches, and independent agencies and institutions of higher education... that surplus, transfer, trade-in, otherwise dispose of, or replace electronic media resources in the Commonwealth.
  - – Applies to equipment owned or leased by the agency.
  - - Offered only as guidance to local government entities.

Data Removal Standard – Background

- All electronic media containing Commonwealth data, whether stored on Commonwealth assets or that of a service provider, shall have all of that Commonwealth data securely removed from the electronic media as specified by this standard before the electronic media is surplused, transferred, traded-in, otherwise disposed of, or replaced.

- This standard applies to all electronic media that has memory such as
  - hard drives of personal computers
  - Servers and mainframes
  - Personal Digital Assistants (PDAs)
  - Routers, firewalls, and switches
  - Tapes, diskettes, CDs, DVDs
  - Worm devices
  - Printers
  - Universal Serial Bus (USB) data storage devices

Data Removal Standard – General Steps

- Before all data is completely erased or otherwise made unreadable in accordance with this standard; however, the data must be reviewed and processed for retention in accordance with the agency's records retention policy.
- Electronic media shall be securely erased at the earliest time after being taken out of use but not later than 60 days.
- The effectiveness of the data removal process shall be tested by a quality assurance function independent of the organizational unit performing the data removal.
- After the removal of Commonwealth data from the electronic media is complete, the process shall be certified.

Data Removal Standard – Removal Methods

- There are 3 acceptable methods for removing data
  - Overwriting
  - Degaussing
  - Physical Destruction

- Clearing data (deleting files) removes information from electronic media in a manner that renders it unreadable. However, because the clearing process does not prevent data from being recovered by technical means, it is **not** an acceptable method of removing Commonwealth data from agency or service provider hard disk storage media.

Data Removal Standard – Overwriting

- Overwriting of data means replacing previously stored data on a drive or disk with a predetermined pattern of meaningless information.
- A minimum of one pass of the entire device for a 15 GB or greater drive.
- A minimum of three passes of the entire device for drives smaller than 15 GB.
- Sectors not overwritten shall be identified and if they cannot be removed overwriting is not acceptable and another method must be employed.

Data Removal Standard – Degaussing

- Degaussing is a process whereby the magnetic media is erased.
- Hard drives seldom can be used after degaussing.
- Use extreme care when using degaussers as this equipment can cause damage to nearby telephones, monitors, and other electronic equipment.
- Hard disk platters shall be in a horizontal direct during the degaussing process.

Data Removal Standard – Physical Destruction

- Hard drives shall be destroyed when they are defective or cannot be repaired or Commonwealth data cannot be removed for reuse.

- Remove the hard drive from the cabinet and cut the electrical connection. The hard drive should then be subjected to physical force (pounding with a sledge hammer) or extreme temperatures (incineration) that will disfigure, bend, mangle or otherwise mutilate.

- Multiple holes drilled into the hard disk platters is an optional method of destruction

Data Removal Standard – Non-Volatile Memory

- Electronic devices that hold user data or configurations in non-volatile memory shall have all Commonwealth data removed by either the removal of the battery or electricity.

- Other method as recommended by the manufacturer for devices where the battery is not removable.

Data Removal Standard – Other Media

- Examples of other media include, but are not limited to, tapes, diskettes, CDs, DVDs, worm devices, and USB data storage devices.

- Disintegration, incineration, pulverization, shredding or melting are acceptable means of destruction.

- Flash drives may be overwritten with a three pass minimum.

- Diskettes, CDs, DVDs, Tape backups may be degaussed or destroyed.

Data Removal Standard – QA and Testing

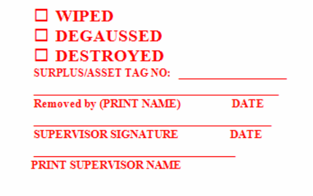
- Effectiveness of the data removal process shall be tested by a quality assurance function independent of the organizational unit performing the data removal.
- If more than one device has had the data removed, a sample of each device type can be tested as opposed to testing every device.
- The sample size for each device type should be commensurate with the sensitivity and risk of the type of data stored but must be at least 10% of the total number of devices for each type of electronic media.
- Testing must be performed within 1 week of the data removal.
- The testing must be documented including date, tester(s), total number of devices in the lot, number tested, method of testing and the result.

Data Removal Standard – Certification

- The data remover must document the data removal including certifying that the data has been effectively removed.

- Documentation to include:
  - The type of equipment/media.
  - The date of the data removal.
  - The method(s) used to expunge the data.
  - The name of the person removing the Commonwealth data.
  - The name and signature of their supervisor.

- One certification tag (Appendix A) may be completed for each physically aggregated lot by affixing the certification tag to the box or shrink wrapped pallet.

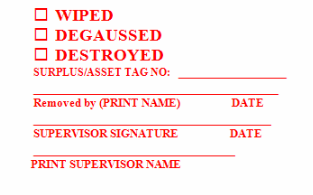


☐ WIPED
☐ DEGAUSSED
☐ DESTROYED
SURPLUS/ASSET TAG NO: ______________

Removed by (PRINT NAME) DATE

SUPERVISOR SIGNATURE DATE

PRINT SUPERVISOR NAME

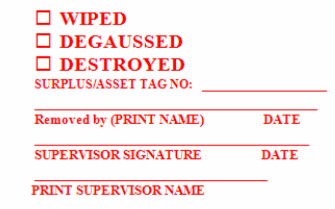


☐ WIPED
☐ DEGAUSSED
☐ DESTROYED
SURPLUS/ASSET TAG NO: ______________

Removed by (PRINT NAME) DATE

SUPERVISOR SIGNATURE DATE

PRINT SUPERVISOR NAME



☐ WIPED
☐ DEGAUSSED
☐ DESTROYED
SURPLUS/ASSET TAG NO: ______________

Removed by (PRINT NAME) DATE

SUPERVISOR SIGNATURE DATE

PRINT SUPERVISOR NAME

Data Removal Standard – Maintenance / Warranty

- It is necessary to protect data on computer hard drives that malfunction and require maintenance or replacement under warranty.
- If the hard drive malfunctions and data can be removed, the drive may be returned to the supplier for replacement under warranty or maintenance.
- Hard drives that are inoperable and do not allow data to be removed, shall be physically destroyed.

Data Removal Standard – Data Recovery

If recovery of data contained on an electronic storage media is required, the agency must provide adequate controls commensurate with the sensitivity of the data contained on the storage media as follows:

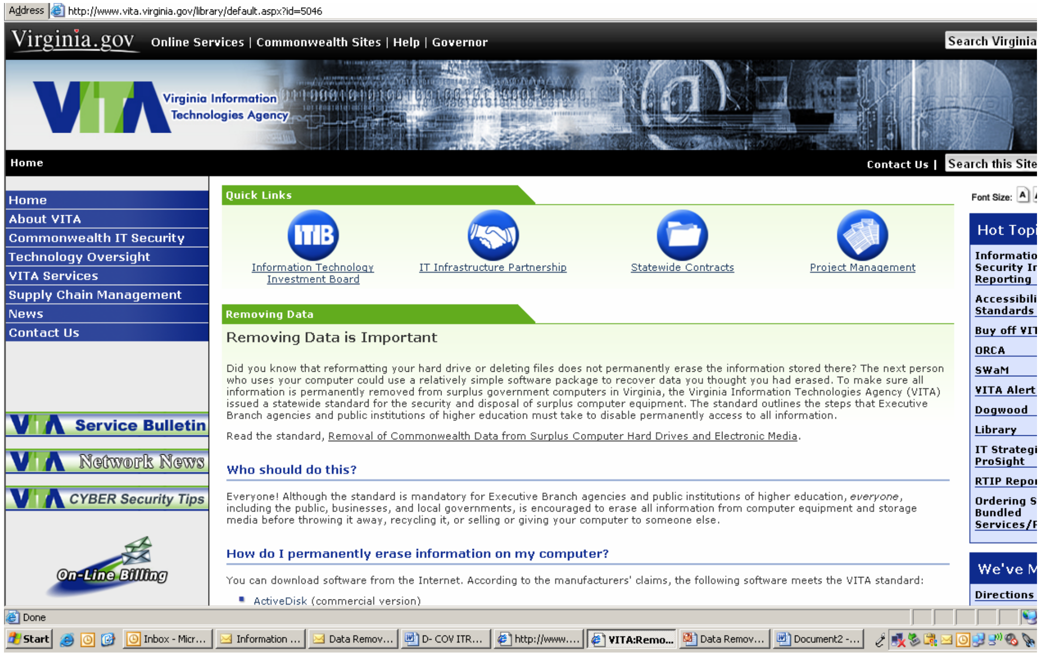
- If a third party is used to recover the data, the agency must ensure that requirements for data protection as outlined in the Policy and Standard are adhered to.

- The agency may require a non-disclosure agreement and/or confidentiality agreement in order to strictly enforce the privacy of the data.

- If the media must be removed from the agency premises and sent offsite for recovery, the agency must ensure that the vendor provides a secure facility and safeguarding capabilities such as background checks, etc. to address handling and processing requirements of sensitive information.

Data Removal Standard – Removal Software

- The list of recommended software may be viewed at the following URL: http://www.vita.virginia.gov/library/default.aspx?id=5046



Removing Data

Removing Data is Important

Did you know that reformatting your hard drive or deleting files does not permanently erase the information stored there? The next person who uses your computer could use a relatively simple software package to recover data you thought you had erased. To make sure all information is permanently removed from surplus government computers in Virginia, the Virginia Information Technologies Agency (VITA) issued a statewide standard for the security and disposal of surplus computer equipment. The standard outlines the steps that Executive Branch agencies and public institutions of higher education must take to disable permanently access to all information.

Read the standard, Removal of Commonwealth Data from Surplus Computer Hard Drives and Electronic Media.

Who should do this?

Everyone! Although the standard is mandatory for Executive Branch agencies and public institutions of higher education, *everyone*, including the public, businesses, and local governments, is encouraged to erase all information from computer equipment and storage media before throwing it away, recycling it, or selling or giving your computer to someone else.

How do I permanently erase information on my computer?

You can download software from the Internet. According to the manufacturers' claims, the following software meets the VITA standard:

- ActiveDisk (commercial version)

Questions

Virginia Information Technologies Agency

§2.2-2009 Information Security Annual Report

Cathie Brown, CISM, CISSP
Deputy Chief Information Security Officer

Requirement

C. The CIO shall report to the Governor and General Assembly by December 2008 and annually thereafter, those executive branch and independent agencies and institutions of higher education that have not implemented acceptable policies, procedures, and standards to control unauthorized uses, intrusions, or other security threats. For any executive branch and independent agency or institution of higher education whose security audit results and plans for corrective action are unacceptable, the CIO shall report such results to the (i) Information Technology Investment Board, (ii) affected cabinet secretary, (iii) Governor, and (iv) Auditor of Public Accounts. Upon review of the security audit results in question, the Information Technology Investment Board may take action to suspend the public bodies information technology projects pursuant to subdivision 3 of § 2.2-2458, limit additional information technology investments pending acceptable corrective actions, and recommend to the Governor any other appropriate actions.

Simplified Summary

WHAT: Commonwealth Information Security Annual Report
WHEN: December, 2008 and annually thereafter
WHO: Executive Branch and Independent agencies and institutions of higher education

REPORT:

Bodies who have not implemented acceptable policies, procedures, and standards to control unauthorized uses, intrusions, or other security threats and Security audit results and plans for corrective action that are unacceptable to the Information Technology Investment Board (ITIB), affected Cabinet Secretary, Governor and Auditor of Public Accounts (APA)

POTENTIAL CONSEQUENCES:

Upon review of the audit results in question, the ITIB may take action to suspend the public bodies information technology projects, limit additional IT investments pending acceptable corrective actions, and recommend to the Governor any other appropriate actions.

Process Overview

- Verify the list of agencies and institutions
- Identify data points for assessment
- Vet our plan with APA
- Assess and analyze data
- Work with agencies on inadequate findings
- Draft report
- Finalize report changes
- Submit to Chief Information Officer (CIO)

Proposed Data Points

- Official ISO Designation
- ISO Attendance at ISO Orientation
- IT Security Audit Plan Submission
- Results of audits including 3rd Party and APA Audits
- Corrective Action Plans (CAPs)
- IT Security Policy & Std Exceptions on file
- IT Security Incidents and Resolutions

Examples of "Acceptable"

- ISO is designated
- IT Security Audit plan has been submitted
- CAP's address audit points and are submitted quarterly
- Exceptions have adequate mitigating controls and are current

Questions

VITA Virginia Information Technologies Agency

Wireless Threats and Best Practices

802.11 - Cellular Data - Bluetooth

Tripp Sims

Commonwealth of Virginia Security Architect

Questions & Comments: tripp.sims@vita.virginia.gov

Content

- ***Why Worry On Wireless?***
- **IEEE 802.11 Wireless LAN**
  - Threats, Best Practices
- **Cellular Data**
  - Threats, Best Practices
- **Bluetooth**
  - Threats, Best Practices
- **Questions and Comments**

Why Worry on Wireless?

Wireless assets are by their very nature, more subject to theft, eavesdropping, and abuse.

- **Assets which are mobile on a regular basis are far more likely to get lost or stolen from unsecured locations.**

- **Assets which communicate via RF (radio frequency) are going to leak signal.**

- **And finally infrastructure assets which allow communication via RF are simply unable to verify the validity of all the RF signals they will see.**

Due to these inherent insecurities assets which communicate wirelessly are viewed with a more critical security eye and typically must conform to more rigorous security requirements than non-wireless assets.

What is IEEE 802.11 or WLAN?

Most specifically IEEE 802.11 is a set of specification by the Institute of Electrical and Electronic Engineers for Wireless Local Area Networks.

These specifications include the following popular wireless networking standards in order, by release date: 802.11a, 802.11b, 802.11g, and 802.11n.

Wired Equivalency Protocol (WEP), intended to provide the confidentiality of wired networks, was included in the 1999 802.11 draft. In 2001, The University of California, Berkeley presented a paper describing weaknesses in the WEP. Later in 2001 AT&T researchers publicly presented a valid WEP attack. In 2003 the Wi-Fi alliance announced that WEP had been superceded by Wi-Fi Protected Access (WPA). And finally in 2004 the IEEE announced that WEP had been depreciated with the ratification of 802.11i (WPA2).

IEEE 802.11 Wireless LAN

Real World 802.11 WLAN Threats

- WEP and WPA Personal have been proven to be entirely ineffective security measures for 802.11 WLANs.
- Rogue Access Points continue to be a significant risk to production network environments.
- WPA-PSK and WPA2-PSK (Pre-Shared Key) offline dictionary attacks.
- Multiple and varied Denial of Service attacks.

IEEE 802.11 WLAN Best Practices

- At a minimum, in a wireless network that terminates in your LAN, employ WPA2 Enterprise utilizing an Extensible Authentication Protocol such as:

  PEAPv0/EAP-MSCHAPv2, EAP-TLS or EAP-TTLS/MSCHAPv2

- Always utilize an encrypted (SSL/IPSEC/L2TPv3) VPN to connect to a Commonwealth network remotely through a Commonwealth “Hot Spot” WLAN. Consider utilizing a VPN through wireless networks employing the prescribed mechanisms above.

- Never broadcast SSIDs.

- Consider utilizing a Wireless Intrusion Detection System (WIDS).

- Ensure communication between wireless clients is blocked.

Cellular Data - Phones and Data Cards

Real World Cellular Phone Threats

- Theft of service or personal/corporate information from lost or stolen device.
- Theft of service or personal/corporate information from duplicated SIM.
- Older cellular phones (typically 800Mhz non-digital) are still prone to low-technology eavesdropping.
- Cell phones “tethered” to PCs for use as wireless modems tend to drop the user directly on to the Internet.

Cellular Data - Phones and Data Cards

Real World Cellular Data Card Threats

- Theft of service or personal/corporate information from lost or stolen device.
- Once a device is registered very little information is needed to utilize the device in another computer.
- Cellular data cards typically drop their users directly onto the Internet.
- As a result users typically cannot take advantage of corporate security measures until they make VPN connection.

Cellular Data Best Practices

- Never utilize a cellular data card or ‘tethered’ cellular phone in your laptop without the use of a personal firewall, AntiVirus, and preferably host integrity checking software.
- Never store corporate data on your cellular phone. Only store personally identifiable information on your cellular phone if you must and only then if it can be encrypted and password protected.
- Seriously consider the risks of downloading software to your Smartphone or wireless PDA.
- Always report a lost or stolen device immediately.

What is Bluetooth?

Bluetooth is a specification for wireless Personal Area Networks (PANs). Bluetooth provides for networking between laptops, cellular telephones, PCs, printers, game consoles, PDAs, digital cameras and a wide range of other personal devices.

This communication takes place over a secure globally unlicensed radio frequency.

Bluetooth is quickly becoming a ubiquitous service available in cars, radios, cell phones, laptops, and PDAs - and is used in 'pairings' between all of these devices to synchronize information between them.

Unfortunately there have been historical deficiencies in the implementation of security on Bluetooth enabled devices. The first report vulnerability in Bluetooth was in 2003 and was related to deficiencies in Bluetooth implementation. In 2004 a pairing of Bluetooth devices was made between two devices over a mile away from each other. In 2005 Cambridge University researchers published a paper detailing passive attacks against PIN protected pairings.

Bluetooth

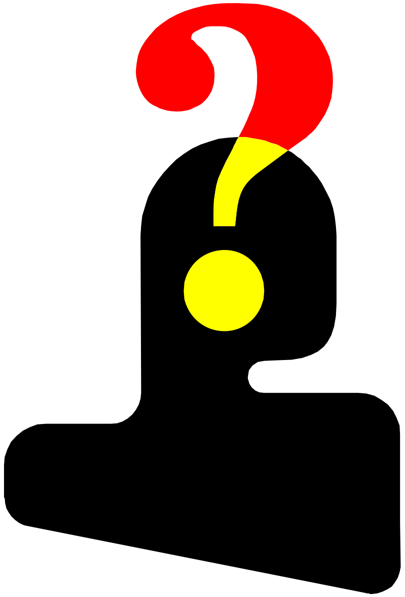
Real World Bluetooth Threats

- Man-in-the-Middle attacks are possible against insecure implementations of Bluetooth.
- Devices with weak or improperly configured security controls are subject to being taken over, being message bombed, and having their information stolen.
- Proof of concept has shown that devices utilizing insecure implementations of Bluetooth could be subject to worm propagation.

Bluetooth Best Practices

- If you don't have an active need for Bluetooth services, ensure the device or peripheral is disabled.
- If you have a need to pair Bluetooth devices ensure the utilization of a strong PIN just as you would a strong password for your personal information.
- When configuring a Bluetooth a service attempt to ensure that only the most minimal services needed are configured. Restrict connectability, discoverability, and pairability as much as possible.
- Always utilize the strongest authentication available.

Questions and Comments



UPCOMING EVENTS!

Wednesday, January 9, 2008 General Assembly Session

Thursday, January 10, 2:00 – 4:00 ISO Orientation CESC ISO orientation is a small group exploration of Information Security in the Commonwealth focusing on the COV IT Security Policy and Standards and is open to all Commonwealth ISO's and interested IT persons!

- To register email VITASecurityService@VITA.Virginia.gov

Tuesday, January 22, 8:30 – 11:00 - AITR Meeting CESC

Tuesday, January 22, 12:00 - 2:00 p.m. IS Council Meeting with committee meetings from 2:00 – 3:00 CESC

- To register email VITASecurityService@VITA.Virginia.gov

UPCOMING EVENTS!

!NEXT ISOAG MEETING!

Wednesday, February 6

1:00 – 4:00

@ CESC Unless We Receive an Offer of Another Venue!

UPCOMING EVENTS!

March 3-8 2008 - SANS at Virginia Tech

These classes are available to state and local government employees including state and local law enforcement at a substantial discount. The registration URL is http://www.cpe.vt.edu/isect.

The price is $700/person for the entire event. Topics include: PCI Compliance, Advanced Network Worm and Bot Analysis, Windows Command-Line Kung Fu In-Depth and Reverse-Engineering Malware. Many thanks to Randy Marchany, Va Tech IT Security Lab Director for letting us know about this opportunity!

UPCOMING EVENTS!

March 10 - 15 2008 - SANS at the Association of College and University Auditors (ACUA) in Jacksonville, Florida

AUDIT 507: Auditing Networks, Perimeters & Systems; is a six-day course and begins with a high-level introduction on methods and assessment programs. Five of the six days in the course will include hands-on exercises with the demonstrated tools on a live in-class network. Each student is required to bring their own laptop to class which will allow you to experiment with the tools discussed in class and to actually perform review functions against SANS-provided servers in class.

The class offers 36 CPE at a significantly reduced rate of $1,500 for the entire event. GIAC Certification is available for an additional charge. The class is being held at the Hyatt Regency Riverfront hotel in the heart of the downtown business, entertainment, and sports district. . For more information and to register, visit: http://www.acua.org/go/events-and-seminars/sans-institute

Other Business

OTHER BUSINESS - IREC

Information Risk Executive Council (IREC) Renewal!

Based on the votes from our Information Security Officers we will be renewing the Commonwealth of Virginia subscription to the Information Risk Executive Council (IREC). This membership allows every Commonwealth of Virginia employee to register and use the services. The tools and papers include those around topics such as Information Security Awareness, Identity and Access Management, Information Protection and more!

Please register by going to: https://www.irec.executiveboard.com/Public/Register.aspx

For questions or problems, please contact:
Jennifer Smith - (202) 587-3601
jsmith@executiveboard.com

OTHER BUSINESS

Any Other Business?

ADJOURN

THANK YOU FOR ATTENDING!!

ENJOY